NC DPH BioTerrorism and Disease Surveillance Overview

Integrating/Developing
Core Systems for
NEDSS and HAN

Control, Testing, Surveillance and Response

Preliminary Draft Document – 2/22/02

National Electronic Disease Surveillance System (NEDSS)

- 100% Java (SDK 1.3.1)
- J2EE Compliant
- Requires High Availability
- Requires Tight Security & External Access
- SilverStream Application Server Based (Microsoft Version)
- MS SQL Server
- Interface with CDC (Digital Certificate)

Health Alert Network (HAN)

- Requires High Availability
- Requires Tight Security and External Access
- High Band Width Connectivity to all 86 NC Local Heath Departments
- Secure Reporting
- Escalation Based Alert Capability (E-mail, Pager, Fax)
- Distant learning

Open Architecture

- Well-defined Encapsulated, Shared, Services
- Defined Protocols Act as Glue For Aggregation
- Centrally Administered and Maintained
- Effortless Sharing of Data and Resources
- Extensible, Scalable, Heterogeneous
- Easier for Disaster Recovery Efforts
- Cost Effective (Both Short and Long Term)
- Common Solution Design, Open Standards
- Off-the-shelf Components

Open Architecture (Continued)

- Portable Design Tools
- Defacto and Approved Industry Standards
- Union of Services Instead of After Market Middleware
- Platform, OS and Vendor Independence
- Enterprise Portal Supplies Initial Interface for All DPH Offerings
- Simpler Single Sign-On (SSO) Facility

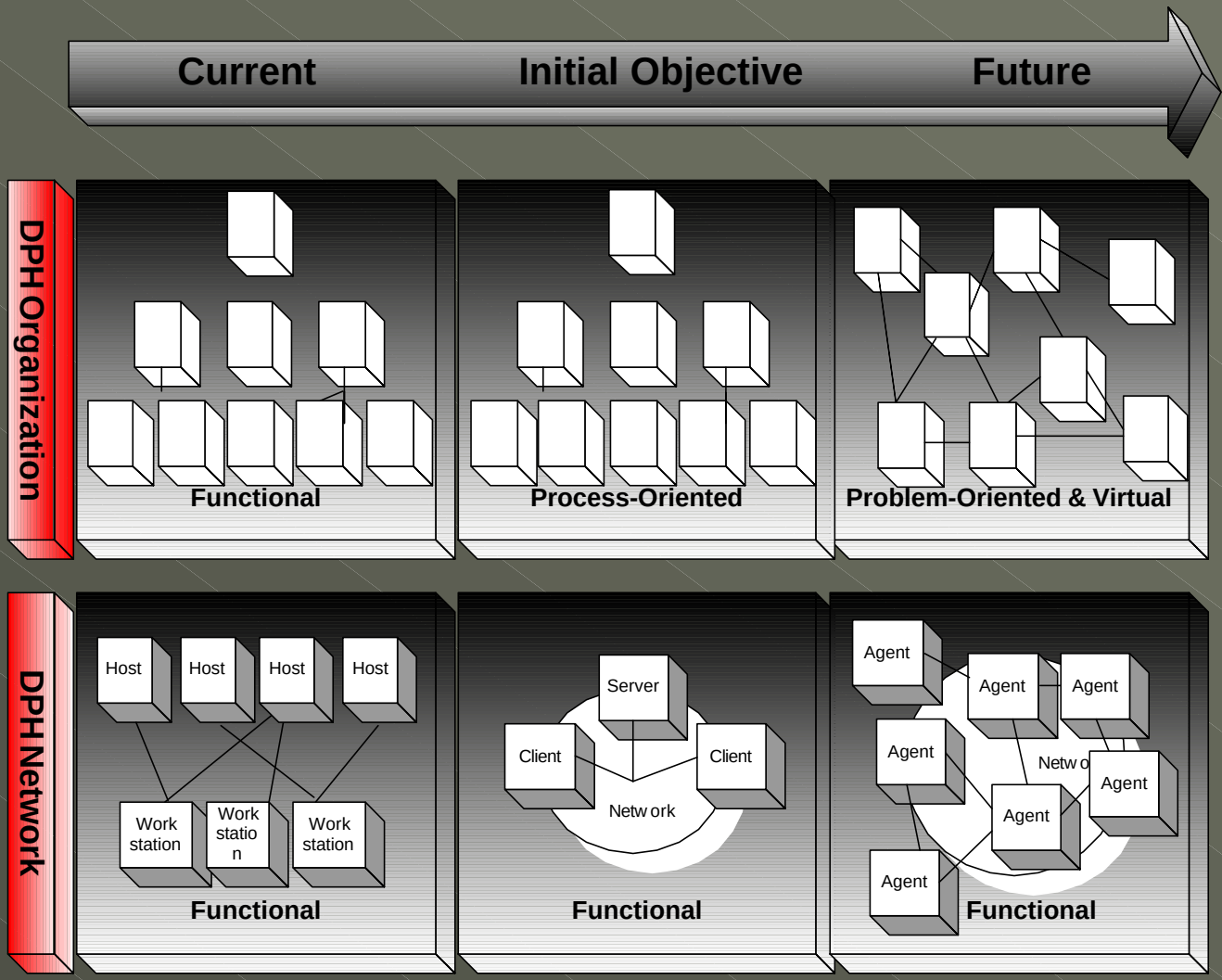
Security Challenges

- Provide Secure “Anywhere” Access to Alerts and Reports (Certificates vs. SSL vs. Other)
- Physical, Authentication, SSO, Filters, etc.
- Internal and External Threats
- Providing Mobile and Remote Connectivity
- Leverage Internet to Lower WAN Costs
- Secure Network’s Performance, Reliability and Availability
- Defining and Enforcing User-Level Security Policies Across your Network
- Immediately Detecting and Responding to Attacks and Suspicious Activity
- Implementing an Open Security Solution that Enables Integration with Industry-Leading and Custom Applications

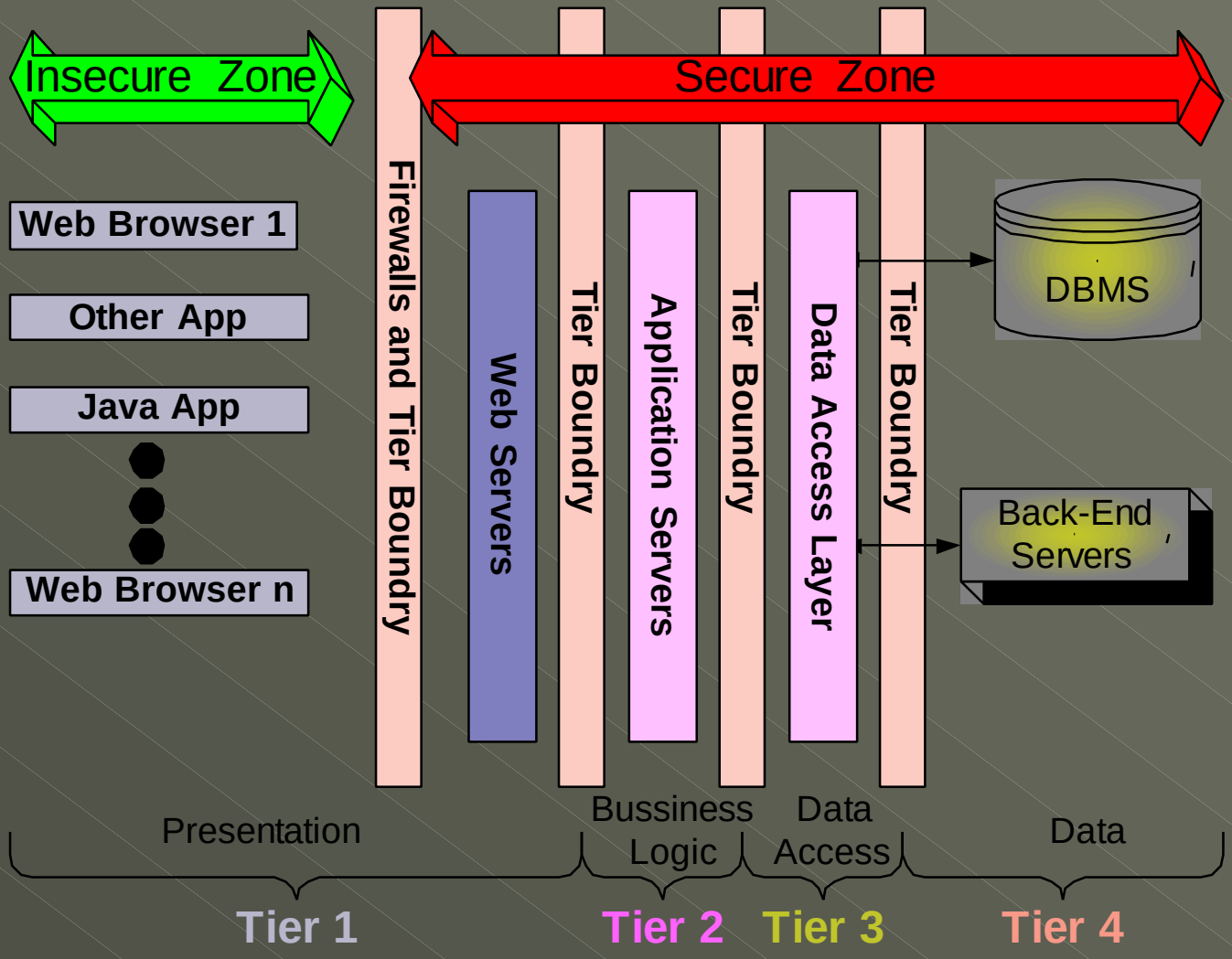
Security Goals

- Best Effort Intrusion Proofing and Monitoring
- Maintaining Servers (Patches, Hot fixes, Updates, Consistent Vulnerability Testing, etc.)
- Verify the Identities of Network Users
- Encrypt Sensitive Data in Transit
- Optimize the Use of Registered IP Addresses
- Apply Security to the Content of Network Traffic
- Detect and Respond to Attacks in Real Time
- Provide Complete Audit Information
- Access Filters Based on User Profiles
- Security Filters to Enforce Privacy on Need-to-Know Basis
- Using Failure Mode and Effects Analysis (FMEA)/Failure Modes and Impacts Criticality Analysis (FMICA) to Verify Infrastructure

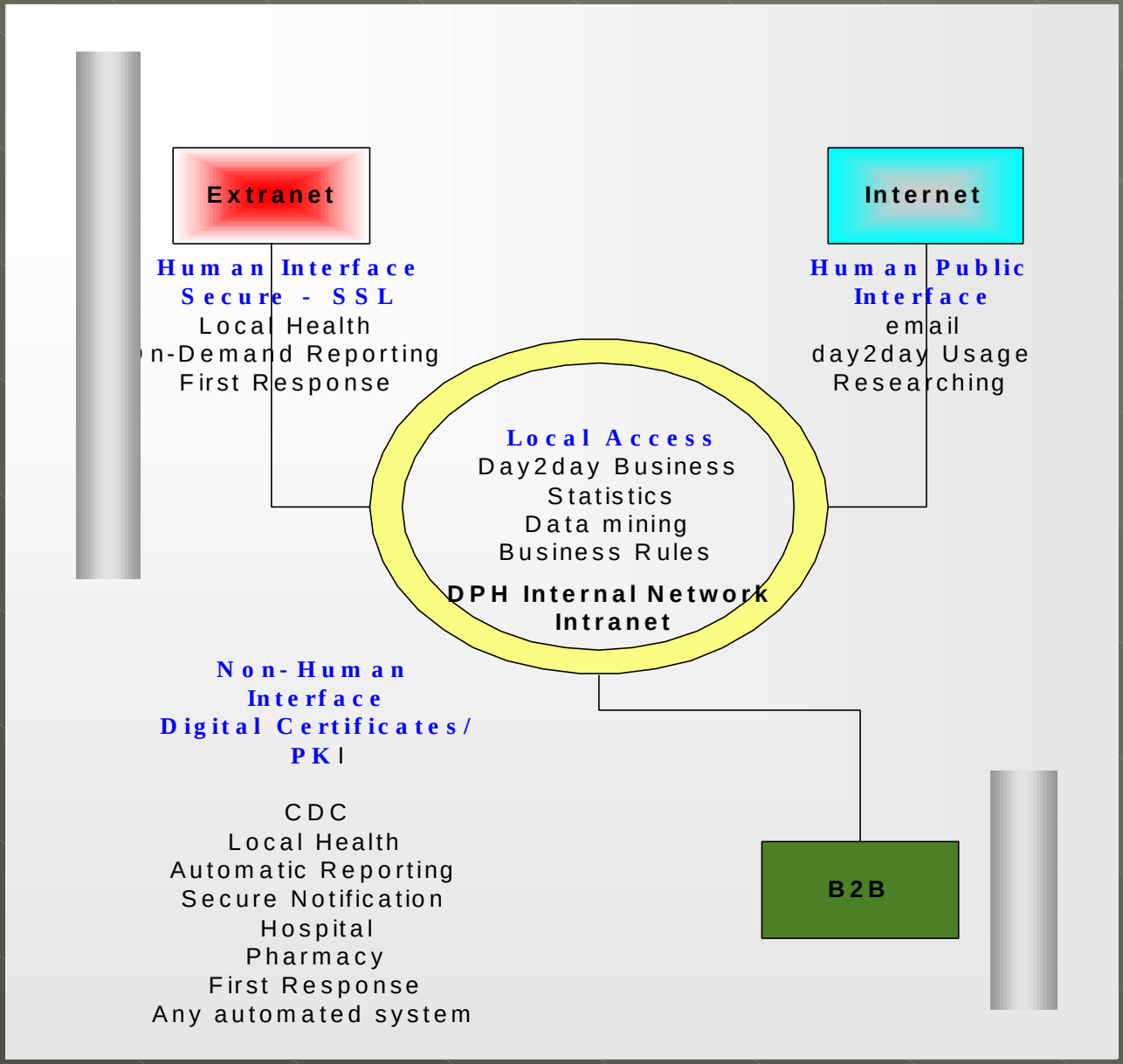
DPH Enterprise Direction



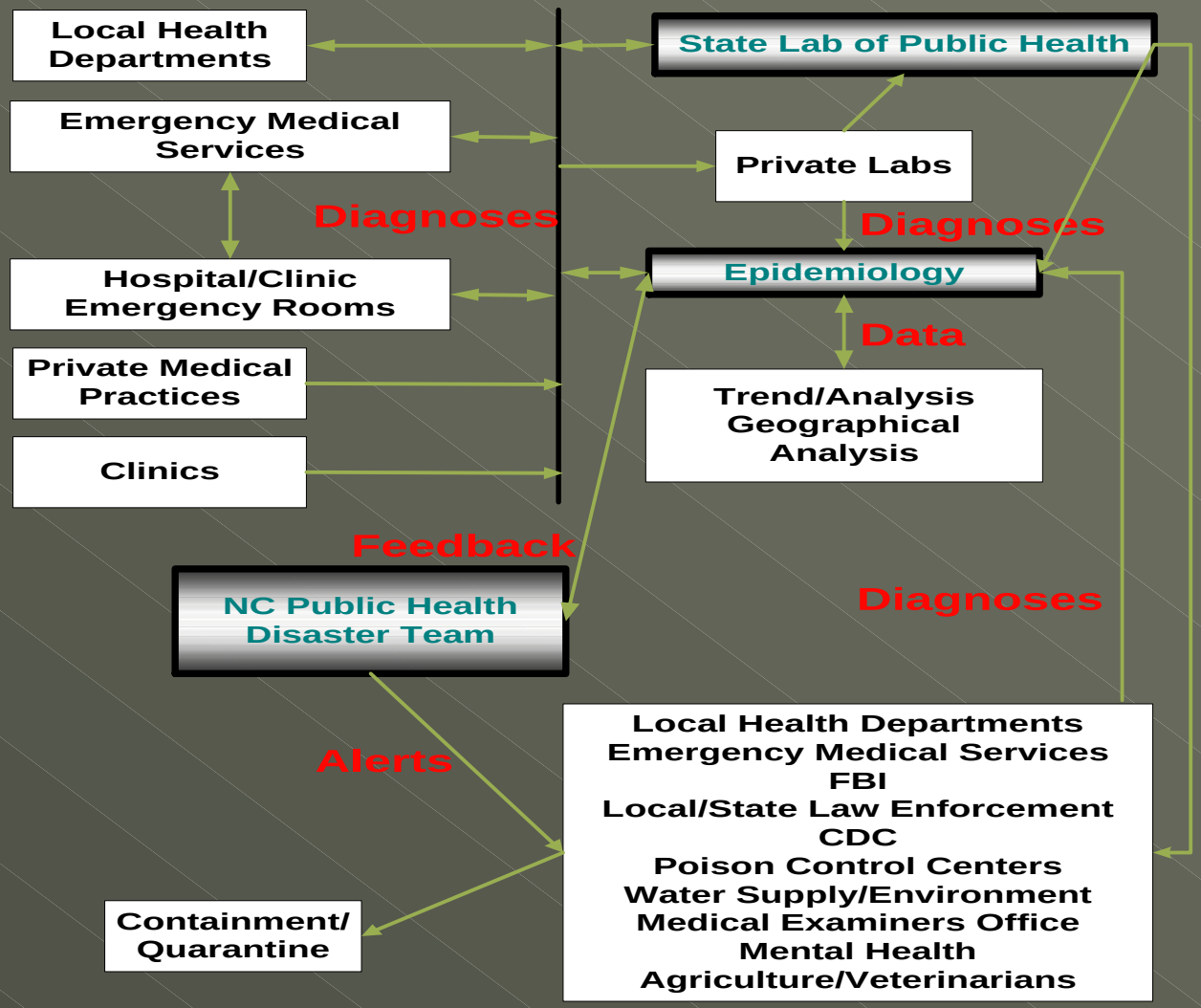
N-Tiered Multi-level Design



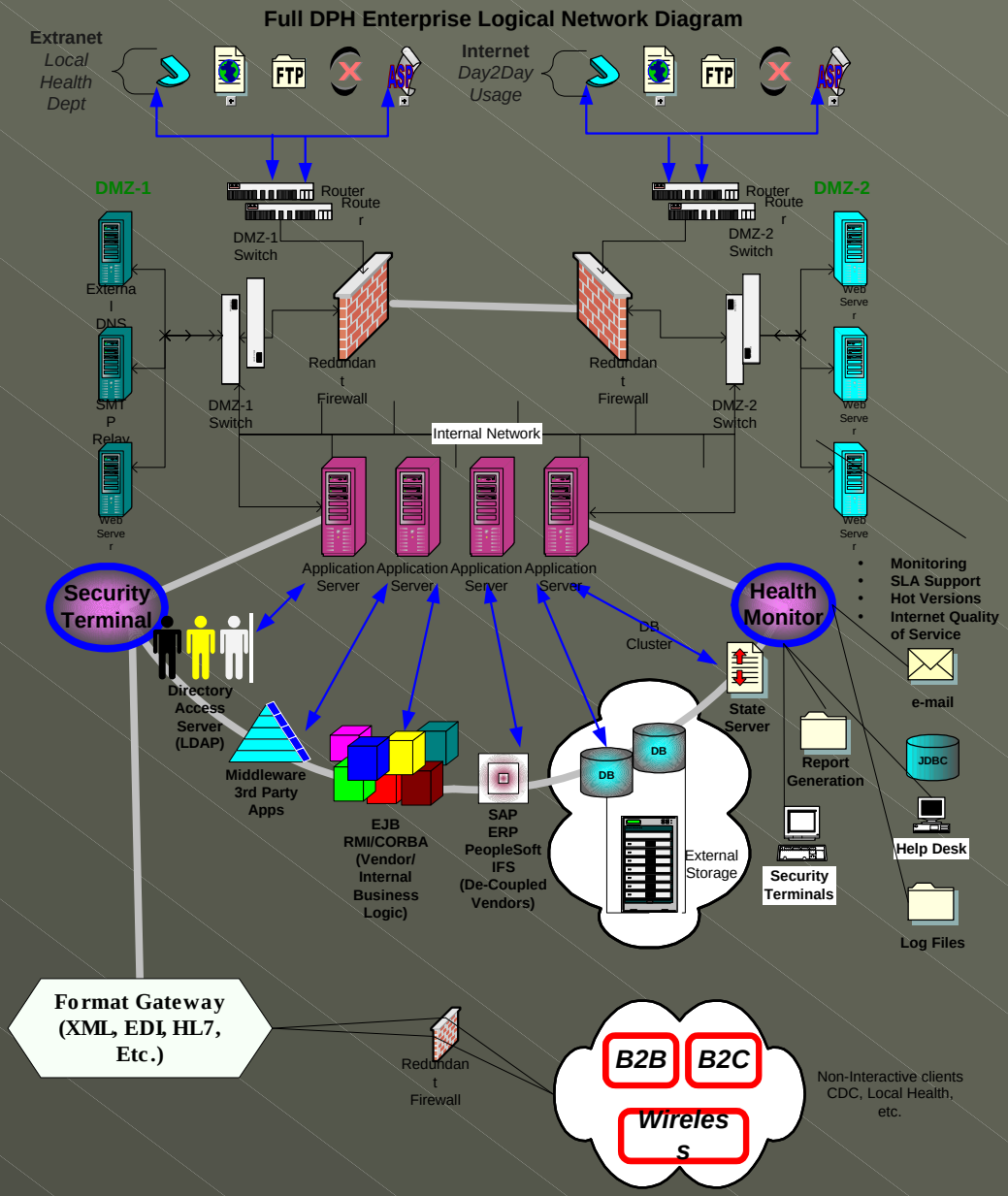
Conceptual Usage



Information Flow



Logical Enterprise Architecture



NEDSS Objectives

- NEDSS Base System is Being Developed and Distributed by the CDC
- Anticipated Availability is June, 2002
- Installation Will Take Place Upon Receipt
- No Additional Development Effort the First Year, Efforts Will Be Focused On:
  - Training
  - Support
  - Administration
- Infrastructure must be in place upon delivery

HAN Objectives

- Develop “Positive Test Results” Data Collection Capability. Will be Replaced by NEDSS When Operational
- Develop Alert and Notification Capability
- Develop Core Reporting Capability
- Base System Must be Operational by July, 2002